Notice of Allowability	**Application No.** 09/521,646	**Applicant(s)** HATAKEYAMA ET AL.
	Examiner Daniel L. Greene	**Art Unit** 3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9/3/2004*.

2. ☒ The allowed claim(s) is/are *1-16*.

3. ☒ The drawings filed on *08 March 2000* are accepted by the Examiner.

4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
      1. □ Certified copies of the priority documents have been received.
      2. □ Certified copies of the priority documents have been received in Application No. _____ .
      3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *10/27/2004* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with James K. Folker on 10/27/2004.

The application has been amended as follows:

7. A content usage control system which controls the usage of content supplied by an authorized information supplier including a content producer who is also an information producer and persons authorized by the information producer, said system comprising:

a user unit which requests usage of the content, and decodes the encrypted content using a content decode key in the case of satisfying license conditions obtained by decoding license information, that is encrypted in a multiplex way in a predetermined order, sent in accordance with a content usage request, based on ID information of the physical elements of the user unit when the license information is passed to each of the physical elements in sequence, said user unit including a plurality of physical elements;

a setting unit which sets a license expressed as a structure by a combination of logic sums and logic products of a plurality of partial licenses for the content based on the ID information of the physical elements of said user unit including media used in said user unit and ID information for the user;

a conditions storage unit, which stores the license conditions, set by said setting a holding unit which holds said content decode key;

an extraction unit which receives the content usage request from said user unit and extracts the license conditions and said content decode key corresponding to said user unit; and

a production unit which produces the license information by encrypting the license conditions and said content decode key based on the ID information of the physical elements through which the license information is passed in sequence until the content is decoded by use of the content decode key and sends the license information to said user unit;

wherein the license information is partially decoded by one of said physical elements, ~~in inverse to said predetermined order~~, in inverse to said predetermined order, and then said partially decoded license information is sent to another of said physical elements to be decoded.

12. A program, encoded in a computer readable medium, executed by a computer of a content usage apparatus connected to a network for enabling a user to use the content, said program being intended to perform operations comprising the steps of:

electronically transmitting ID information of physical elements of said content usage apparatus and ID information of the user to an external content management apparatus, which manages the content in accordance with a content usage request;

determining license conditions and a content decode key by decoding license information, that is encrypted in a multiplex way in a predetermined order, transmitted by said external content management apparatus in response to the content usage request, using the ID information of the physical elements of said content usage apparatus when the license information is passed to each of the physical elements in sequence; and

electronically decoding the content using the content decode key when permitted upon determination of the license conditions;

wherein the license information is partially decoded by one of said physical elements, in inverse to said predetermined order, and then said partially decoded license information is sent to another of said physical elements to be decoded.

13. A content usage method employed on a content usage apparatus connected to a network for enabling a user to use the content, said method comprising:

electronically transmitting ID information of physical elements of said content usage apparatus and ID information of the user to an external content management apparatus, which manages the content in accordance with a content usage request;

electronically determining license conditions and a content decode key by decoding license information, that is encrypted in a multiplex way in a predetermined order, transmitted by said external content management apparatus in response to the content usage request, using the ID information of the physical elements of said content usage apparatus when the license information is passed to each of the physical elements in sequence; and

electronically decoding the content using the content decode key when permitted upon determination of the license conditions;

wherein the license information is partially decoded by one of said physical elements, in inverse to said predetermined order, and then said partially decoded license information is sent to another of said physical elements to be decoded.

14. A program, encoded in a computer readable medium, executed by a computer of a content usage apparatus for enabling a user to use the content, said program being intended to perform operations comprising the steps of:

electronically determining, in response to a content usage request, license conditions and a content decode key by decoding license information, encrypted in a multiplex wav in a predetermined order, of the content based on ID information of physical elements of said content usage apparatus when the license information is passed to each of the physical elements in sequence; and

electronically decoding the content using the content decode key when permitted upon determination of the license conditions;

wherein the license information is partially decoded by one of said physical elements, in inverse to said predetermined order, and then said partially decoded license information is sent to another of said physical elements to be decoded.

15, A content usage method employed on a content usage apparatus for enabling a user to use the content, said method comprising:

electronically determining, in response to a content usage request, license conditions and a content decode key by decoding license information, that is encrypted in a multiplex way in a predetermined order, of the content based on ID information of physical elements of said content usage apparatus when the license information is passed to each of the physical elements in sequence; and

electronically decoding the content using the content decode key when permitted upon determination of the license conditions;

wherein the license information is partially decoded by one of said physical elements, in inverse to said predetermined order, and then said partially decoded license information is sent to another of said physical elements to be decoded.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

The following is an examiner's statement of reasons for allowance:

As per claims 1, 7, 8, 9, 10, 11, 12, 13, 14, 15, taken either individually or in combination with other prior art of record fails to teach or suggest component assembly that controls access to data.

Specifically, both the Ginter et al. reference and the Iwayama et al. reference fail to disclose or suggest the decoding of license information using the ID information of a plurality of physical elements in which "the license information is partially decoded by a first one of said physical elements," and "then said partially decoded license information is sent to another of said physical elements to be decoded," as defined in the independent claims.

As described on page 10 (line 21) through page 11 (line 3) of the present Specification, one problem to be resolved by the present invention is to prevent illegitimacy overlooked in the case where the license is produced from the usage environment specifying physical element, where the usage environment specifying physical element is simply a large sized device, and part of the device is illegitimate. The present invention prevents such illegitimacy by decoding the license partially by each of the physical elements, wherein the partially decoded license information is moved from one physical device to at least one other physical device for the decoding to be completed.

Ginter et al. reference teaches that multiple pieces of independently managed VDE content can be combined into a single VDE container object; that the combination of VDE managed pieces will frequently require securely deriving content control requirements (including combination rules); and that "Figures I-J teaches about "component" assembly that controls access to data."

However, the teachings mentioned above still lack any disclosure or suggestion that the encrypted license information should be partially decoded within one of the physical elements, and then the partially decoded license information is sent to another physical element to complete the decoding. Initially, in the discussion of component assemblies in columns 79-87, the Ginter et al. reference does not mention decoding the component assemblies. Instead, the discussion of decoding (decrypting) the encrypted information is found in column 67, inter alia. Column 67 of Ginter et al. refers to decrypting information using a special purpose encrypt/decrypt hardware engine 522 (shown in Figure 9 within hardware tamper resistant barrier 502, which is also shown in Figure 10). Thus, the complete decoding (decrypting) appears to take place within a single component (hardware engine 522). There is no disclosure or suggestion that the decoding (decrypting) should take place within two (or more) different physical components, as in the present invention. Further, there is no disclosure or suggestion that the decoding should partially take place within one physical component, and that the partially decoded license information should be moved to a second physical component for completing the decoding of the license information.

With regard to the component assemblies shown in Figures I I I and 11 J of the Ginter et al. reference, even assuming that each of the various separate components and/or the various component sub-assemblies that make up the component assembly include license information that is to be decoded, there is no disclosure or suggestion that even a single piece of license information is to be partially decoded in one physical element, and then that partially decoded license information is to be moved to a different physical element to complete the decoding. Instead, Figures 11 I and 11 J appear to simply show that as long as the component assembly has been assembled in an authorized manner, it can be loaded and the components can be used.

The Examiner further argued that layering security techniques is not novel, and that mere duplication of a working part involves only routine skill in the art. However, the claimed invention is more than either the mere layering of known security techniques or the mere duplication of a working part. The present invention does not relate to merely duplicating the concept of decoding encrypted license information by requiring that multiple licenses be decoded by multiple physical elements. Instead, as mentioned earlier, the license information is partially decoded by one physical element, and the partially decoded license information is passed to another physical element for the decoding to be completed. In this manner, the license information is not fully decoded unless all physical elements have authorization. In the case where multiple licenses are decoded by multiple physical elements, certain licenses can be fully decoded (and perhaps used elsewhere), even though there are unauthorized physical elements within the system.

Finally, the present invention seems to be similar to a situation of requiring opening of multiple doors with multiple separate keys. However, a more accurate analogy would be having a single key and at least two doors, where the key is placed within the first door, and the key is somewhat modified by the first door before placing the modified key into the second door, where, if the modified key is authorized for the second door, it then opens both doors.

More specifically, one example of an embodiment of the present invention that includes this feature is shown in Applicants' Figure 14, which is described on page 41 of the present application. In this embodiment of the license decoding process, the encrypted license includes, among other things, the ID's of the following physical elements --the storage device (device serial number 141), the medium (medium serial number 143), and the reproduction device (ID of reproduction device 144).

Briefly, when the correct conditions are present, the encrypted license information is partially decoded by the storage device 140, and the partially decoded license is sent to the reproduction device 144, which in turn completes the process of decoding the license. More specifically, in this embodiment, the license generated by the license server 40 has been encrypted by encrypting the access control list (ACL) and the content decode key (Kc) using the key Kp, which is the physical element ID of the reproduction device 144. Using, as a key, the value of the exclusive OR of the DSN 141 and the MSN 143, has further encrypted the license. During decoding, the storage device 140 first reads the MSN 143, and the exclusive OR is calculated between it and DSN 141, whereby the license is partially decoded into {ACL, Kc}Kp. The partially decoded license is then sent to the reproduction device 144, which completes the decoding process of the partially decoded license using the key Kp, which is comprised of the physical element ID of the reproduction device 144. If the access conditions have been satisfied, the content decode key Kc can then be used to decode the content, and the reproduction device can reproduce the decoded content.

In contrast, in the device of Ginter et al., license information does not appear to be partially decoded by a first physical device, nor does any partially decoded information appear to be passed through to a second physical device for final decoding and use. Instead, full decoding appears to take place by referencing each physical device separately, without passing license information through one physical device to a second physical device.

To remedy this deficiency, the Examiner relied upon the Iwayama et al. reference. However, the Iwayama et al. reference also fails to disclose or suggest a device in which license information is partially decoded by a first physical device, and where the partially decoded information is then sent to a second physical device for final decoding and use. As described in column 9 (line 37) through column 10 (line 37) of the Iwayama et al. reference, while making reference to Figure 1, all of the decoding in this device appears to occur within a single physical element (the information transforming (converting) section 1), and there is no disclosure or suggestion of partially decoding license information, nor of sending partially decoded license information to another physical device.

More specifically, in the system of the Iwayama et al. reference, the information transforming (converting) section 1 retrieves encoded data content and encoded content ID information from the data storing section 3. Then, the information transforming (converting) section 1 receives encoded utilization permission information from the utilization-permitting device 2, and the information transforming (converting) section 1 decodes the encoded utilization permission information to generate a decoding key. The information transforming (converting) section 1 uses that decoding key to decode the encoded data content and the encoded content ID information. The user compares the decoded content ID information against the content ID information input, and if they coincide, the decoded data content is output to the user. Although the Iwayama et al. reference teaches a plurality of physical elements, in the Iwayama et al. reference, all decoding takes place within a single one of those physical elements. - Thus, the Iwayama et al. device fails to disclose or suggest partial decoding of license information, where a portion of the decoding takes place in one physical element and that partially decoded license information is sent to another physical element for additional decoding.

Claims 2-6 are dependent upon Claim 1 and thus has all the limitations of claim 1 and is allowable for that reason.

Claim 16 is dependent upon Claim 15 and thus has all the limitations of claim 15 and is allowable for that reason.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Greene whose telephone number is 703-306-5539. The examiner can normally be reached on M-Thur. 8am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P. Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

11/04/2004

DLG

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600